



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/458,922	12/10/1999	MOHAMMAD PEYRAVIAN	P-4541.003	9481
24112	7590	06/01/2004	EXAMINER	
COATS & BENNETT, PLLC P O BOX 5 RALEIGH, NC 27602			WU, ALLEN S	
		ART UNIT		PAPER NUMBER
		2135		
DATE MAILED: 06/01/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/458,922	PEYRAVIAN ET AL.
	Examiner Allen S. Wu	Art Unit 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 05 March 2004.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-30 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-30 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 10 December 1999 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
5) Notice of Informal Patent Application (PTO-152)
6) Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-9, 12-27 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nissl et al (hereinafter Nissl), US Patent 6,530,023, in view of Haber et al (hereinafter Haber), US Patent 5,136,647.

As per claims 1, 13, and 19, Nissl discloses a means of time stamping a document (see for example; abstract) comprising a time stamp receipt including identifying data associated with said document and a time indication (see for example; col 4 ln 50-55), validating said time stamp receipt by comparing the time indication to the current time (see for example; col 2 ln 62-col 3 ln 6 and fig 7) and if time stamp receipt is valid, binding said identifying data and said time indication using a cryptographic binding scheme (see for example; encryption, 3 ln 7-11 and col 7 ln 42-59). Nissl discloses that such time stamping is done in the computer through the use of a plug-in board or ASIC (see for example; col 3 ln 27-36). Nissl further discloses an outside agency for performing data protection. However Nissl is silent on the specific embodiment of using such an outside agency for performing said time stamping.

Haber et al, discloses a method for time stamping a document (col 2, ln 33-49) comprising of receiving time stamp receipt (certificate, col 3 ln 1-5) including identifying data associated with the document (identity of the author, col 4 ln 3-33) at an outside agency (see for example; TSA fig 1); obtain the current time (adding digital data signifying the current time, col 2 ln 59-66); and binding at said outside agency said identifying data (digital document, col 2 ln 61-66) and a time indication (adding digital data signifying the current time) using a cryptographic binding scheme (applying the agency's cryptographic signature scheme, col 2 ln 66-67 and col 3 ln 1-5). Nissl further discloses such "current time" being received from an external source (see for example; fig 4 and col 2 ln 62-col 3 ln 6). One of ordinary skill in the art at the time of the applicant's invention would have realized such time stamping being done be an outside agency wherein the outside agency supplies the "current time" to validate the time indication (local time) before applying a cryptographic binding. By incorporating such verifying and binding at an outside agency, one would have recognized the increase in security by the use of a central third party as a witness to the binding and also a uniformity of protection by having all documents signed by a central trusted party. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Haber within the system of Nissl because it would have provided increased security and added uniformity.

As for receiving the time indication at an outside agency, Nissl discloses the document being time-stamped with the time of its creation (see for example; col 4 ln 40-49) and that such time is validated before binding (see for example; col 2 ln 62-col 3 ln 6). Haber further discloses the outside agency being able to receive time-stamp receipts from authors/clients including a time indication (see for example; col 8 ln 17-25). One of ordinary skill in the art at the time of the applicant's invention would have realized that such a combination results in the sending of the time indication to be checked at an outside agency.

In further regard to claims 13 and 19, Nissl discloses creating a time stamp receipt including identifying data associated with said document and a time indication (see for example; col 4 ln 50-55). One of ordinary skill in the art at the time of the applicant's invention would have realized such a creation of a time receipt in order to be verified at the outside agency. Haber further discloses the authors creating a time-stamp receipt including data associated with the document and a time indication (see for example; col 8 ln 17-20) and transmitting said time stamp receipt to an outside agency (transmittal may be directly to the author or by way of the administrative TSA, col 5 ln 1-16 and col 8 ln 24-25).

As per claims 2 and 20, Nissl-Haber discloses the claimed limitations above (see claim 1). Nissl further discloses transmitting binding information to a third party (see for example; col 7 ln 60-col 8 ln 7). Haber further discloses transmitting said binding information to a designated party from the outside

agency (transmits the certificate back to the author or by way of the administrative, col 5 ln 4-16).

As per claims 3, 14, and 21, Nissl-Haber discloses the claimed limitations above (see claim 1). Nissl further discloses identifying data comprising a digital representation of at least a portion of said document (see for example; col 5 ln 6-18). Haber et al further discloses the identifying data comprising a digital representation of at least a portion of said document at an outside agency (convert the digital document string to a unique number; col 3 ln 6-24; document is hashed, col 6 ln 1-15).

As per claims 4, 15, and 22, Nissl-Haber discloses the claimed limitations above (see claim 3). Nissl further discloses identifying data comprising a digital sequence derived by application of a deterministic function to at least a portion of said document (see for example; MD5, col 5 ln 7-12). Haber et al further discloses identifying data comprising a digital sequence derived by application of a deterministic function to at least a portion of said document at an outside agency (reduced digital size by means of a deterministic function, col 3 ln 6-24).

As per claims 5, 16, and 23, Nissl-Haber discloses the claimed limitations above (see claim 4). Nissl further discloses digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said

document (see for example; MD5, col 5 ln 7-12). Haber et al further discloses digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document being received by the outside agency (reduced digital size by means of a deterministic function which may, for example, be any one of a number of algorithms known in the art as "oneway hash functions", col 3 ln 6-24; document is hashed, col 6 ln 1-15).

As per claims 6, 17, and 24, Nissl-Haber discloses the claimed limitations above (see claim 1). Haber et al further discloses the time stamp receipt further including an identification number associated with the document originator (the author whose system identification number is 172 in a 1000 member author universe, col 6 ln 8-15). Such document identification number provides for identification of the document originator, which is important when time-stamping through a central trusted authority where multiple users are seeking time stamping of documents. It would have been obvious to one of ordinary skill in the art to further include an identification number of the document originator within the Nissl-Haber combination because it would have increased the authenticity of the time-stamp by allowing the outside agency to authenticate or associate an originator with the time stamp.

As per claims 7, 18, and 25, Nissl-Haber discloses the claimed limitations above (see claim 6). Haber et al further discloses the time stamp receipt further

including a sequential record number (TSA generates a time stamp receipt which includes, for example, a sequential receipt number, col 4 ln 3-33). A sequential record number provides for a means of fixing the time stamp to a order relative to time and thereby increasing it authenticity through added security check of a correct sequential record number. When handling time stamping of a plurality of authors, one of ordinary skill in the art would have realized that such a sequential record number would have added organizational order to the issuing of time stamps. It would have been obvious to one of ordinary skill in the art to further include a sequential record number within the Nissl-Haber combination because it would have increased the authenticity of the time-stamp.

As per claims 8 and 26, Nissl-Haber discloses the claimed limitations above (see claim 7). Haber et al further disclose the step of validating said time stamp receipt includes comparing (comparison of a number, col 4 ln 3-33), said identification number (author, A_k , col 4 ln 3-33) and sequential record number (TSA generates a time stamp receipt which includes, for example, a sequential receipt number, col 4 ln 3-33) with data maintained by the outside agency (comparison of a number of relevant distributed certificates, col 3 ln 3-33).

As per claims 9 and 27, Nissl-Haber discloses the claimed limitations above (see claim 1). Nissl further discloses binding steps including encryption (see for example; col 3 ln 7-10). One of ordinary skill in the art at the time of the

applicant's invention would have realized such a cryptographic signature scheme comprises encryption of data using a key. Haber et al further discloses said binding step including the signing of a combination of said identifying data and said time indication using a digital cryptographic signature scheme at the outside agency (certifies the resulting separate time-stamped receipt with its own verifiable cryptographic signature col 5 ln 1-16).

As per claims 12 and 30, Nissl-Haber discloses the claimed limitations above (see claim 1). Nissl further discloses binding steps including encryption (see for example; col 3 ln 7-10). Haber further discloses binding step including an encryption on a combination of said identifying data and said time indication using a secret key controlled by said outside agency (cryptographic public key scheme to be employed in this example (generally known in the field as the "RSA", signature scheme), col 6 ln 25-35 and col 7 ln 1-24; Haber does not explicitly say the private key is controlled by outside agency. However, the RSA signature scheme is well known in the art to have a public and private key pair. Only the signing party knows the private key. Therefore a secret key controlled by the outside agency is to be inherent to the teachings of Haber). Such key controlling by the outside agency is part of the process done by the outside agency disclosed by Haber and is rejected under the same rationale of claim 1.

3. Claims 10 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nissl et al (hereinafter Nissl), US Patent 6,530,023, in view of Haber et al (hereinafter Haber), US Patent 5,136,647 as applied to claims 1 and 19 above, and further in view of Schneier.

As per claims 10 and 28, Nissl-Haber et al discloses binding at said outside agency said identifying data and said time indication using a cryptographic binding scheme as described above (see claim 1).

Furthermore, Haber teaches a secret key controlled by said outside agency (cryptographic public key scheme to be employed in this example (generally known in the field as the "RSA", signature scheme), col 6 In 25-35 and col 7 In 1-24; Haber does not explicitly say the private key is controlled by outside agency. However, the RSA signature scheme is well known in the art to have a public and private key pair. Only the signing party knows the private key. Therefore a secret key controlled by the outside agency is to be inherent to the teachings of Haber). However the Nissl-Haber combination does not teach that the binding step includes computing a message authentication code on a combination of identifying data and said time indication using a secret key controlled by said outside agency. A message authentication code is a key dependent one-way hash function. Schneier teaches the generation of message authentication codes with secret keys (IBC-Hash, page 457-459). Binding information together is a manipulation of digital data to achieve one representation of the combination of data. To compute message authentication

code, one manipulates the digital data, through the use of one-way hash functions and keys, in such a way as to develop a representation of the combination of data. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Schneier within the Nissl-Haber combination because it would have provided a more secure form of binding information together. Message authentication codes are known to provide authenticity without secrecy since only someone with the identical key can verify the hash.

4. Claims 11 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nissl et al (hereinafter Nissl), US Patent 6,530,023, in view of Haber et al (hereinafter Haber), US Patent 5,136,647 as applied to claims 1 and 19 above, and further in view of Levine et al, US Patent 6,393,566.

As per claims 11 and 29, Nissl-Haber discloses binding at said outside agency said identifying data and said time indication using a cryptographic binding scheme as described above (see claim 1). However, the Nissl-Haber combination does not teach that the binding step includes computing a hash value on a combination of identifying data and said time indication. Levine et al teaches the use of hashing algorithms to bind time indication information and identifying data (col 4 In 1-8). Binding the identifying data and time indication data is a manipulation of digital data. The use of hash algorithms to produce such a binding of data into a representation is well known in the art. It would

have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Levine within the Nissl-Haber combination because it would have added another way of binding the information for the time stamp receipt. Hash algorithms are well known in the art to produce a secure fingerprint of data. Computing a hash value as part of the binding step increases the security of the time stamp from unwanted activity.

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. Claims 1-30 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-26 of copending Application No. 09/458928 (hereinafter '928 application). Although the conflicting claims are not identical, they are not patentably distinct from each other.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

As per claims 1, 13, and 19 of the instant application, claims 1 and 14 of the '928 application recite similar means of receiving a time stamp receipt, binding of identifying data and time indication. Claims 1 and 14 of '928 does not explicitly teach validating said time stamp receipt at said outside agency by comparing the time indication in said time stamp receipt. Claims 1 and 14 of '928 application recites the computing the age of said time stamp receipt. In making such a computation, one of ordinary skill in the art at the time of the applicant's invention would have realized that a comparison of the time indication and current time would have been made. Claim 14 of the '928 application further recites certification of a received time stamp receipt by the outside agency. It would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to validate said time stamp receipt by comparing the time indication in said time stamp receipt to the current time because it would have increased authenticity of the time stamp receipt at binding at the outside authority. By comparing the time indication in the receipt with a current time, the outside agency can further validate that the time stamp is received within a certain tolerance, thus increasing authenticity of the time stamp certification by the outside agency by ensuring that all certified time stamp receipts meet more requirements.

In further regards to claims 13 and 19 of the instant application, claim 14 of the '928 application further recites the similar limitation of creating a time stamp receipt and transmitting said time stamp receipt.

Claims 2-12 and 20-30 of the instant application recites similar limitations of claims 2-7, 9-13, 15-20, and 22-26 of the '928 application.

Claims 14-18 of the instant application recites similar limitations of claims 16-20 of the '928 application.

Response to Arguments

7. Applicant's arguments, see page 2, filed March 5, 2004, with respect to the rejection(s) of claim(s) 13-19 under 35 USC 102 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of a different interpretation of previous cited art.

8. Applicant's arguments, see pages 2-3, filed March 5, 2004, with respect to the rejection(s) of claim(s) 1-9, 12, and 19-30 under 35 USC 103 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of a different interpretation of previous cited art.

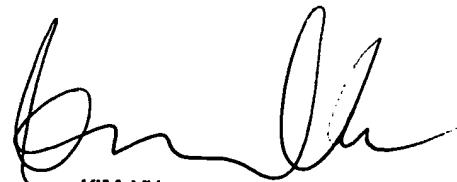
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen S. Wu whose telephone number is 703-305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Allen Wu
Patent Examiner
Art Unit 2135



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2135